Adding denied sessions to session table

Blocking the packets of a denied session can take more CPU processing resources than passing the traffic through. By putting denied sessions in the session table, they can be kept track of in the same way that allowed session are so that the FortiGate unit does not have to reassess whether or not to deny each of the packets on an individual basis. If the session is denied all packets of that session are also denied.

In order to configure this to take place you will need to configure 2 CLI settings.

ses-denied-traffic

This setting determines whether or not the firmware includes denied session in the session table. The default of this setting is "disable" so it needs to be enabled.

block-session-timer

This setting sets the length of time, in seconds, that the session is kept in the table. The range is from 1 to 300 seconds. The longer the session is in the table the less potential for impact on the CPU but the greater the amount of memory taken up holding the information in the table.

The following is an example configuration:

```
config system setting
    set ses-denied-traffic enable
    set block-session-timer 60
    end
```